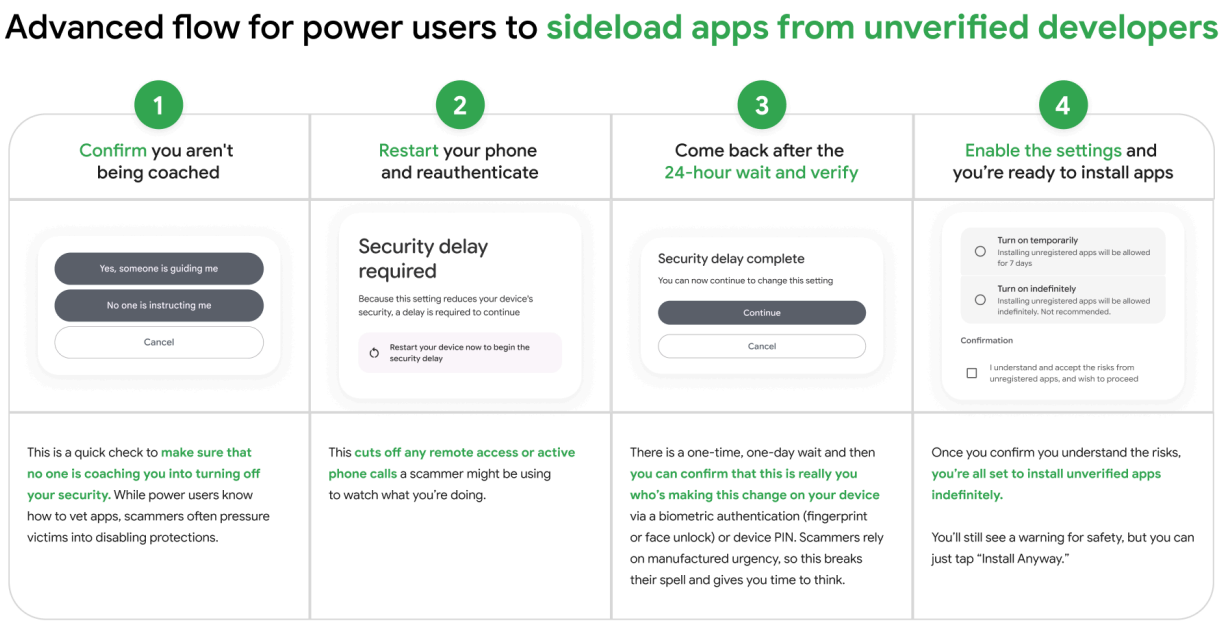
Google details new 24-hour process to sideload unverified Android apps

arstechnica.com/gadgets/2026/03/google-details-new-24-hour-process-to-sideload-unverified-android-apps/

March 19, 2026


Advanced flow for power users to sideload apps from unverified developers
1
Confirm you aren't being coached
Yes, someone is guiding me
No one is instructing me
Cancel
This is a quick check to make sure that no one is coaching you into turning off your security. While power users know how to vet apps, scammers often pressure victims into disabling protections.
2
Restart your phone and reauthenticate
Security delay required
Because this setting reduces your device's security, a delay is required to continue
Restart your device now to begin the security delay
This cuts off any remote access or active phone calls a scammer might be using to watch what you're doing.
3
Come back after the 24-hour wait and verify
Security delay complete
You can now continue to change this setting
Continue
Cancel
There is a one-time, one-day wait and then you can confirm that this is really you who's making this change on your device via a biometric authentication (fingerprint or face unlock) or device PIN. Scammers rely on manufactured urgency, so this breaks their spell and gives you time to think.
4
Enable the settings and you're ready to install apps
Turn on temporarily
Installing unregistered apps will be allowed for 7 days
Turn on indefinitely
Installing unregistered apps will be allowed indefinitely. Not recommended.
Confirmation
I understand and accept the risks from unregistered apps, and wish to proceed
Once you confirm you understand the risks, you're all set to install unverified apps indefinitely.
You'll still see a warning for safety, but you can just tap "Install Anyway."

Google is planning big changes for Android in 2026 aimed at combating malware across the entire device ecosystem. Starting in September, Google will begin restricting application sideloading with its developer verification program, but not everyone is on board. Android Ecosystem President Sameer Samat tells Ars that the company has been listening to feedback, and the result is the newly unveiled advanced flow, which will allow power users to skip app verification.

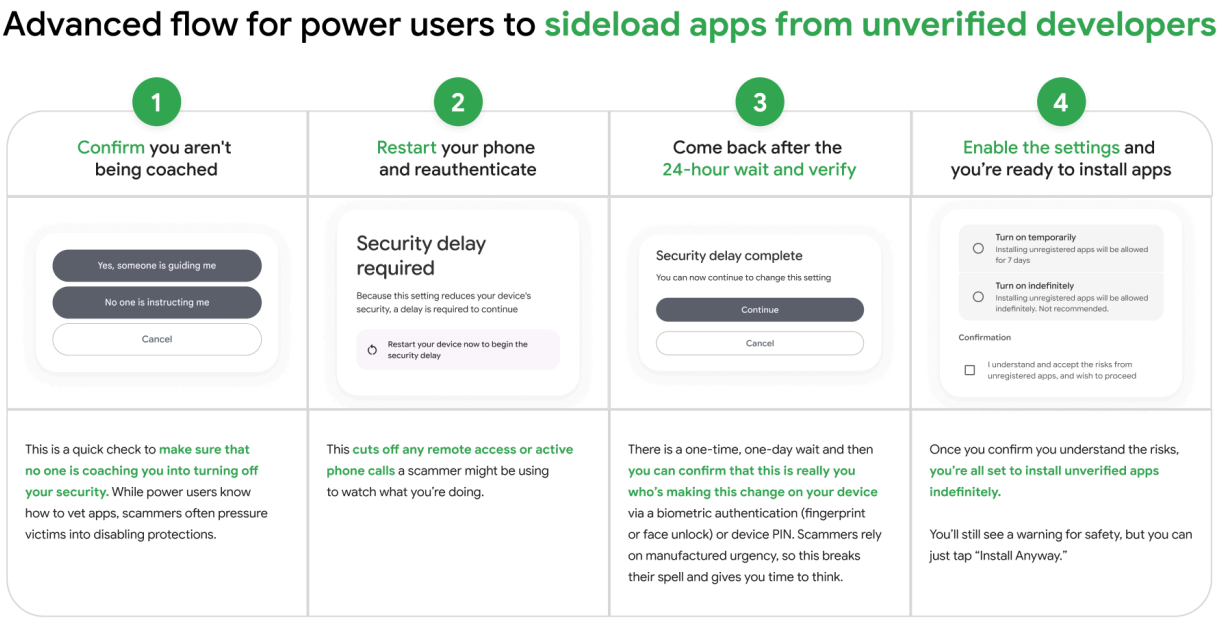
With its new limits on sideloading, Android phones will only install apps that come from verified developers. To verify, devs releasing apps outside of Google Play will have to provide identification, upload a copy of their signing keys, and pay a $25 fee. It all seems rather onerous for people who just want to make apps without Google's intervention.

Apps that come from unverified developers won't be installable on Android phones—unless you use the new advanced flow, which will be buried in the developer settings.

When sideloading apps today, Android phones alert the user to the "unknown sources" toggle in the settings, and there's a flow to help you turn it on. The verification bypass is different and will not be revealed to users. You have to know where this is and proactively turn it on yourself, and it's not a quick process. Here are the steps:

- Enable developer options by tapping the software build number in About Phone seven times
- In Settings > System, open Developer Options and scroll down to “Allow Unverified Packages.”
- Flip the toggle and tap to confirm you are not being coerced
- Enter device unlock pin/password
- Restart your device
- Wait 24 hours
- Return to the unverified packages menu at the end of the security delay
- Scroll past additional warnings and select either “Allow temporarily” (seven days) or “Allow indefinitely.”
- Check the box confirming you understand the risks.
- You can now install unverified packages on the device by tapping the “Install anyway” option in the package manager.

The actual legwork to activate this feature only takes a few seconds, but the 24-hour countdown makes it something you cannot do spur of the moment. But why 24 hours? According to Samat, this is designed to combat the rising use of high-pressure social engineering attacks, in which the scammer convinces the victim they have to install an app immediately to avoid severe consequences.


Advanced flow for power users to sideload apps from unverified developers
1
Confirm you aren't being coached
Yes, someone is guiding me
No one is instructing me
Cancel
This is a quick check to make sure that no one is coaching you into turning off your security. While power users know how to vet apps, scammers often pressure victims into disabling protections.
2
Restart your phone and reauthenticate
Security delay required
Because this setting reduces your device's security, a delay is required to continue
Restart your device now to begin the security delay
This cuts off any remote access or active phone calls a scammer might be using to watch what you're doing.
3
Come back after the 24-hour wait and verify
Security delay complete
You can now continue to change this setting
Continue
Cancel
There is a one-time, one-day wait and then you can confirm that this is really you who's making this change on your device via a biometric authentication (fingerprint or face unlock) or device PIN. Scammers rely on manufactured urgency, so this breaks their spell and gives you time to think.
4
Enable the settings and you're ready to install apps
Turn on temporarily
Installing unregistered apps will be allowed for 7 days
Turn on indefinitely
Installing unregistered apps will be allowed indefinitely. Not recommended.
Confirmation
I understand and accept the risks from unregistered apps, and wish to proceed
Once you confirm you understand the risks, you're all set to install unverified apps indefinitely.
You'll still see a warning for safety, but you can just tap "Install Anyway."

You’ll have to wait 24 hours to bypass verification.
Credit: Google

You’ll have to wait 24 hours to bypass verification. Credit: Google

“In that 24-hour period, we think it becomes much harder for attackers to persist their attack,” said Samat. “In that time, you can probably find out that your loved one isn’t really being held in jail or that your bank account isn’t really under attack.”

But for people who are sure they don’t want Google’s verification system to get in the way of sideloading any old APK they come across, they don’t have to wait until they encounter an unverified app to get started. You only have to select the “indefinitely” option once on a phone, and you can turn dev options off again afterward.

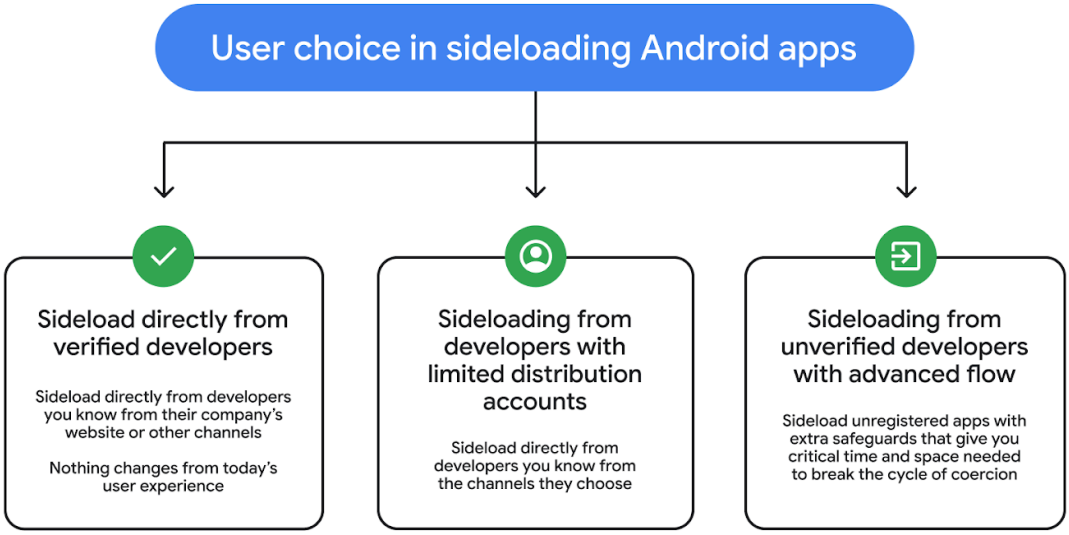
Choice vs. security

According to Samat, Google feels a responsibility to Android users worldwide, and things are different than they used to be with more than 3 billion active devices out there.

“For a lot of people in the world, their phone is their only computer, and it stores some of their most private information,” Samat said. “Over the years, we’ve evolved the platform to keep it open while also keeping it safe. And I want to emphasize, if the platform isn’t safe, people aren’t going to use it, and that’s a lose-lose situation for everyone, including developers.”

But what does that safety look like? Google swears it’s not interested in the content of apps, and it won’t be checking proactively when developers register. This is only about identity verification—you should know when you’re installing an app that it’s not an imposter and does not come from known purveyors of malware. If a verified developer distributes malware, they’re unlikely to remain verified. And what is malware? For Samat, malware in the context of developer verification is an application package that “causes harm to the user’s device or personal data that the user did not intend.”

So a rootkit can be malware, but a rootkit you downloaded intentionally because you want root access on your phone is not malware, from Samat’s perspective. Likewise, an alternative YouTube client that bypasses Google’s ads and feature limits isn’t causing the kind of harm that would lead to issues with verification. But these are just broad strokes; Google has not commented on any specific apps.


User choice in sideloading Android apps
Sideload directly from verified developers
Sideload directly from developers you know from their company's website or other channels
Nothing changes from today's user experience
Sideloading from developers with limited distribution accounts
Sideload directly from developers you know from the channels they choose
Sideloading from unverified developers with advanced flow
Sideload unregistered apps with extra safeguards that give you critical time and space needed to break the cycle of coercion

Google says sideloading isn't going away, but it is changing.
Credit: Google

Google says sideloading isn't going away, but it is changing. Credit: Google

Google is proceeding cautiously with the verification rollout, and some details are still spotty. Privacy advocates have expressed concern that verification will create a database that puts independent developers at risk of legal action. Samat says that Google does push back on judicial orders for user data when they are improper. The company further suggests it's not intending to create a permanent list of developer identities that would be vulnerable to legal demands. We've asked for more detail on what data Google retains from the verification process and for what length of time.

There is also concern that developers living in sanctioned nations might be unable to verify due to the required fee. Google notes that the verification process may vary across countries and was not created specifically to bar developers in places like Cuba or Iran. We've asked for details on how Google will handle these edge cases and will update if we learn more.

Rolling out in 2026 and beyond

Android users in most of the world don't have to worry about developer verification yet, but that day is coming. In September, verification enforcement will begin in Brazil, Singapore, Indonesia, and Thailand. Impersonation and guided scams are more common in these regions, so Google is starting there before expanding verification globally next year. Google has stressed that the advanced flow will be available *before* the initial rollout in September.